最後更新日期：2021 年 6 月 22 日

資料處理附錄

本《資料處理附錄》（「**DPA**」）是《林肯電氣公司最終使用者許可協定》（「**EULA**」）的附錄，適用於林肯電氣公司（「**資料處理者**」）和 EULA 規定的授權使用者（「**資料控制者**」）（各稱以下稱為「**一方**」，統稱為「**雙方**」）之間。

鑒於

EULA 規定了授權使用者使用授權應用程式以及林肯電氣公司提供的其他在線服務（若適用）之權利。為履行 EULA 規定的義務，林肯電氣公司應代表授權使用者擔任資料處理者。為確保遵守個人資料法規，雙方同意補充 EULA，以規定適用於資料處理者代表資料控制者處理個人資料的條款和條件。

雙方特此約定如下：

1. 定義

1.1 在本 DPA 中，以大寫字母表示術語應具有以下含義，除非 EULA 中定義或根據上下文另有要求：

「**資料控制者**」	是指確定個人資料處理目的和方式的實體；
「**資料處理者**」	是指代表資料控制者處理個人資料的實體；
「**資料主體**」	是指其個人資料正在被處理的已識別或可識別身份的個人；
「**指示**」	是指資料控制者向資料處理者提供的指示，以根據 EULA 提供的服務處理個人資料；
「**個人資料**」	是指與已識別或可識別身份的個人有關的任何資訊；可識別身份的個人是可以直接或間接識別其身份的人，特別是透過參考身份標識符，例如姓名、身份證號碼、位置資料、在線標識符，或其特定的一個或多個身體、生理、遺傳、心理、經濟、文化或社會身份等因素；
「**個人資料洩露**」	是指違反安全導致意外或非法破壞、丟失、更改、未經授權披露或訪問已傳輸、存儲或以其他方式處理的個人資料；
「**處理**」	是指對個人資料執行的任何操作，例如收集、記錄、組織、存儲、改編或更改、檢索、諮詢、使用、透過傳輸、傳播、轉移或以其他提供方式進行披露、整理或組合、限制、刪除或銷毀；
「**處理服務**」	是指資料處理者對與 EULA 相關的個人資料進行的處理；
「**特殊類別的個人資料**」	是指揭示種族或民族血統、政治觀點、宗教或哲學信仰、或工會、協會或基金會成員身份、外表、刑事定罪和安全措施、財務和財產資訊、行蹤資訊或信用資訊的任何個人資料，以及處理基因資料、用於唯一識別自然人的生物特徵資料、健康資料、或自然人性生活或性取向資料，或者關於14歲以下未成年人的資料；
「**標準合同條款**」	是指歐盟委員會 2010 年 2 月 5 日以第 2010/87 號決議透過的關於將個人資料傳輸到在第三國設立的處理者的標準合同條款，或雙方商定的任何替代標準條款集。如果資料控制者設立在歐盟以外的司法管轄區，標準合同條款的實體規定中提到的成員國應解釋為資料控制者設立所在的司法管轄區；
「**下級處理者**」	是指資料處理者（或資料處理者的任何其他下級處理者）聘請的按照其指示和書面分包合同的條款代表資料控制者處理個人資料的任何處理者。

1.2 本 DPA 中使用的標題和條款標題僅供參考和方便查閱之用，不屬於本 DPA 的組成部分，並且不得用於解釋本 DPA。

2. 本 DPA 的範圍與適用

2.1 本 DPA 僅補充 EULA 中關於資料處理者根據 EULA 向資料控制者提供的處理服務的規定。

3. 資料處理

3.1 資料處理者同意根據本 DPA 中規定的條款和條件處理個人資料，尤其是資料處理者承諾：

3.1.1 僅代表資料控制者處理個人資料，並始終遵守本 DPA 中定義的資料控制者的指示以及所有適用的資料保護法律；

3.1.2 確保委託履行處理服務的任何人員已承諾保密或承擔適當的法定保密義務；

3.1.3 按照本 DPA 附件 2 的規定，採取技術、物理和組織措施確保個人資料的安全性和機密性，並適當保護代表資料控制者處理的個人資料免遭濫用和丟失；

3.1.4 其將立即通知資料控制者：（a）任何政府主管部門提出的要求披露個人資料的具有法律約束力的請求，除非另有禁止，例如刑法禁止保留執法或情報調查的機密性， （b）影響代表資料控制者處理的個人資料的任何洩露，（c）直接從資料主體收到的任何請求（包括訪問權、更正權、刪除權、反對權、限制權、資料傳輸權以及不受僅基於自動化處理（包括資料畫像）的決定之約束之權利）；資料處理者（i）不會直接回應該請求，除非通知資料主體其正在代表資料控制者實施行為，並向資料主體提供資料控制者的聯繫資訊，以及（ ii）基於到處理的性質，將在可能的情況下透過適當的技術、物理和組織措施協助資料控制者，以履行資料控制者回應資料主體關於行使權利請求的義務；

3.1.5 向資料控制者提供商業上合理的合作，以協助資料控制者履行其承擔與個人資料安全相關的法律義務，例如：向主管監管機構通知個人資料洩露，將此類個人資料洩露通知受影響的資料主體，並且在適用的情況下，基於處理的性質和資料處理者可獲得的資訊，實施資料保護影響評估並與監管機構事先協商；

3.1.6 向資料控制者提供所有必要的資訊，以證明遵守本 DPA 中規定的義務，並且允許和協助由資料控制者或資料控制者委託的其他審計人員進行第6條中所述的審計（包括檢查）；以及

3.1.7 下級處理者履行的任何處理服務將按照第 7 條規定進行。

3.2 關於處理服務，資料控制者將負責遵守適用法律中關於個人資料的處理以及其向資料處理者發出指示的所有要求。特別是但不影響上述基本規定之前提下，資料控制者確認和同意其將全權負責以下事項：（i）個人資料的準確性、品質和合法性；（ii）在收集和使用個人資料時遵守適用法律規定的所有必要的透明度和合法性要求，包括從資料主體或其他方獲得任何必要的同意和授權；（iii）確保資料控制者有權向資料處理者傳輸或提供對個人資料的訪問權，並且資料控制者已提供任何必要的通知，已獲得與該傳輸以及與根據EULA（包括本 DPA ）的條款進行資料處理相關的任何必要的同意和/或授權；以及 （iv）確保其指示符合適用法律。經資料處理者要求，資料控制者應在三（3）個工作日內向資料處理者提供關於此類通知、同意和授權的書面證據。資料控制者不會將任何特殊類別的個人資料輸入到處理服務中，或以其他方式向資料處理者提供任何特殊類別的個人資料，除非資料控制者另行書面同意。如果資料控制者無法履行其在本 DPA 中規定的職責，資料控制者將立即通知資料處理者，不得無故拖延。授權使用者全權負責審查處理服務，包括任何可用的安全文檔和功能，以確定它們是否滿足授權使用者的要求、業務需求和法律義務。

3.3 資料控制者授權資料處理者對根據 EULA 處理的個人資料進行匿名處理，以獲取與使用授權應用程式和林肯產品和設備相關的分析資料。資料處理者對由此產生的統計資料的進一步使用無須獲得資料控制者的事先授權。

4. 國際資料傳輸

4.1 資料控制者在此確認和同意，為了根據 EULA 提供處理服務，資料處理者可以在美國以及資料處理者所在的任何其他國家傳輸和保留個人資料，以提供處理服務。因此，在提供處理服務的過程中，可能有必要將個人資料傳輸到位於資料控制者所在國家以外的資料處理者。如果資料控制者位於歐洲經濟區或瑞士，雙方則承諾將標準合同條款的規定適用於資料控制者（根據標準合同條款作為資料出口方）將人資料傳輸至資料處理者（根據標準合同條款作為資料進口方）。

4.2 如果資料控制者位於歐洲經濟區和瑞士以外，雙方還承諾將標準合同條款的規定適用於資料控制者（根據標準合同條款作為資料出口方）將個人資料傳輸至資料處理者（根據標準合同條款作為資料進口方），但前提是標準合同條款是法律要求的，並且足以滿足關於資料控制者根據EULA將個人資料傳輸至資料處理者的適用資料處理法規要求。

4.3 如果雙方根據本 DPA 第 4.1 條或第 4.2 條規定適用標準合同條款：

4.3.1 標準合同條款的附件1 應在以下基礎上適用：（a）資料出口方：資料控制者，（b）資料出口方：資料處理者，（c）資料主體：資料控制者（授權使用者）的人員，（d）資料類別：與使用資料處理者擁有、許可或管理的產品和設備相關的資料，該等資料由授權應用程式根據 EULA 進行監控，包括註冊資料（即，使用者名和密碼），（e）特殊類別的個人資料：不適用，以及（f）處理操作：根據 EULA 提供處理服務所需的收集、複製、傳輸、存儲、修改、刪除和其他操作。

4.3.2 就標準合同條款附件 2 所述的目的而言，作為資料進口方的資料處理者實施的技術、物理和組織安全措施的描述應在本 DPA 的附件 2 中規定。

4.4 如果標準合同條款根據第 4.1 條或第 4.2 條在雙方之間適用，其條款則將被視為透過引述納入本 DPA，除非雙方根據第 4.5 條將標準合同條款作為獨立文件進行簽訂執行。

4.5 在適用的資料保護法規要求的範圍內，雙方應作為單獨的文件簽訂並執行標準合同條款。

5. 終止

5.1 本 DPA 將在 EULA 生效日期時生效。

5.2 本 DPA 將在（a）EULA 或（b）資料處理者與處理服務相關的義務終止或到期後（以日期在先者為準）自動終止，並且此終止不需要法院命令或法院程式，或者資料處理者、資料控制者或任何其他方採取任何其他行動。在適用的情況下，當本 DPA 終止時，資料處理者應返還資料控制者或按照資料控制者的要求刪除其持有或控制的所有資料控制者的個人資料。經資料控制者要求，資料處理者應以書面方式確認遵守該等義務並刪除所有現有副本，除非適用法律要求存儲或以其他方式允許保留個人資料。

5.3 如果資料處理者嚴重違反或持續違反本 DPA，並且在可以補救的情況下，但是在資料處理者收到資料控制者指明違規且要求補救的通知之日起三十（30）個工作日內未得到補救，資料控制者有權書面通知資料處理者終止本 DPA。

5.4 如果資料控制者嚴重違反或持續違反本 DPA，並且在可以補救的情況下，但是在資料控制者收到資料處理者指明違規且要求補救的通知之日起三十（30）個工作日內未得到補救，資料處理者有權書面通知資料控制者終止本 DPA。

6. 審計與資訊要求

6.1. 在每年不超過一（1）次審計的限度內，並且經資料控制者提前三十（30）天通知后，除非監管機構要求進行審計，資料控制者可在正常上班時間在不會無理干擾資料處理者的業務運營的情況下，親自或指定第三方審計人員（須承擔與該審計相關的保密義務）對資料處理者進行審計。

6.2. 資料處理者應在根據第 6 條進行的審計中給予配合，並向資料控制者提供進行此類審計所需的所有資訊。資料控制者應承擔各方因第 6 條規定的審計而產生的費用和支出。

7. 下級處理者的指定

7.1 僅在履行EULA相關服務所需的情況下，資料控制者授權資料處理者使用在[https://www.lincolnelectric.com/en/Legal-Information/Subprocessors] 可訪問的頁面中列出的下級處理者的服務。

7.2 資料控制者授權資料處理者使用新的下級處理者的服務，但是資料處理者須在下級處理者變更前提前十五（15）天通知資料控制者。如果資料控制者對通知的下級處理者的變更提出異議，資料控制者可以在通知期間內以書面方式終止本 DPA。如果資料控制者未在通知期內終止，則表明資料控制者正式同意下級處理者的變更。

7.3 在任何情況下，如果資料處理者使用下級處理者的服務，下級處理者應透過合同遵守與資料處理者根據本 DPA 處理個人資料相關的同等義務。

8. 其他條款

8.1 對本 DPA 的修訂或補充必須以書面形式進行方可生效。儘管有上述規定，資料處理者可以隨時在不通知資料控制者的情況下修改附件 2 中規定的技術、物理和組織措施，但前提是此修訂不會對個人資料的安全性、機密性或完整性產生重大影響。

8.2. 本 DPA 中提到的「書面」包括電子郵件通信和掛號信件。

8.3 如果本 DPA 的任何條款無效或變得無效，這不會影響其餘條款的有效性。如果本 DPA 的任何條款無效，雙方則應在任何情況下真誠地努力將無效的條款替換為另一項可執行、有效且合法的條款，並且該替代條款應盡可能與原先條款具有相同或等同的法律效力。

8.4 本 DPA 受與 EULA 相同的適用法律管轄。

附件 1 - 司法管轄區特定條款

如果資料控制者在本附件 1 中所列的司法管轄區之一設立，以下條款則應適用於 DPA；如果該等條款與 DPA 的其他規定存在衝突，則應以該等條款為準並替代 DPA 中存在衝突的規定。EULA 中未由本附件中適用的司法管轄區特定條款專門修改的所有條款應保持不變且具有完全效力。

巴西：

雙方確認和同意適用對 DPA 作出的以下修改：

a) DPA 中所有出現的「特殊類別的個人資料」均應取代為「敏感個人資料」。

墨西哥：

雙方確認和同意適用對 DPA 作出的以下修改：

a) DPA 中所有出現的「特殊類別個人資料」均應取代為「敏感個人資料」；
b) 對於標準合同條款的適用，所有提到的個人資料「傳輸」均應解釋為根據墨西哥聯邦關於保護私人持有的個人資料的法律（「*Ley Federal de Protección de Datos Personales en Posesión de los Particulares* 」）進行的個人資料轉發。

俄羅斯：

除 DPA 的規定以外，雙方承諾如下：

a) 資料處理者在此確認，其完全了解根據 DPA 開展的個人資料處理活動的目的僅是提供處理服務，並且應僅出於披露個人資料的目的處理個人資料，而資料控制者需要資料處理者提供的處理服務。此外，當資料控制者要求時，資料處理者應及時以書面方式確認其已遵守此規則。
b) 在向資料處理者披露源自俄羅斯國民的個人資料之前，在以任何方式（包括透過網路）收集此類個人資料時，資料控制者應確保所有此類個人資料已被記錄、系統化、積累、保存、澄清（更新、更改）並使用位於俄羅斯聯邦境內的資料庫進行提取。
c) 如果資料控制者檢測到個人資料的非法處理或不準確，資料控制者應立即指示資料處理者封鎖此個人資料並啟動檢查。受影響的個人資料將在整個檢查期內被封鎖。如果檢查確認個人資料不準確，資料控制者應要求相關資料主體（或其代表）或資料保護機構（若適用）進行修改，並將修改轉發給資料處理者。不準確的個人資料應在相關修改交付給資料控制者之日起七（7）個工作日內儘快進行修改。個人資料一經修改將立即解除封鎖。
d) 如果發現個人資料被非法處理，資料控制者應指示資料處理者在發現之日起三（3）個工作日內停止此類非法處理。如果可能無法消除違規行為並且為了確保個人資料處理的合法性，資料控制者應指示資料處理者在發現之日起十（10）個工作日內銷毀非法處理的個人資料。資料控制者還應通知相關資料主體（或其代表），並在法律要求的情況下通知資料保護機構其已消除違規行為。
e) 如果資料主體撤銷其對個人資料處理的同意，資料控制者應立即通知資料處理者，資料處理者應在資料控制者收到取消通知之日起三十（30）天內停止處理並銷毀此資料主體的個人資料。
f) 如果無法遵守上述 d）項和 e）項規定的期限，資料處理者應在收到資料控制者的要求后，在最長不超過六（6）個的期限內封鎖相關個人資料，並在此期限內銷毀該等個人資料，除非適用法律另有規定。

南非：

雙方確認和同意，對 DPA 的以下修改應適用於 DPA 第 1 條提供的定義：

a) 「資料主體」是指正在被處理的個人資料的擁有主體。
b) 「個人資料」是指 POPIA 中定義的個人資訊，包括與已識別或可識別身份的個人有關的任何資訊。
c) 「POPIA」是指南非 2013 年第 4 號《個人資訊保護法》，以及根據 POPIA 發佈的任何具有約束力的法規、指令、裁決、命令或指南。

<u>美國</u>:

除 DPA 的規定以外，雙方承諾如下：

a) 各方確認和同意，收集和披露傳輸進行處理服務的個人資料（i）不構成，並且任何一方不希望此類活動構成個人資料的銷售，以及（ii）如果授權使用者向資料處理者提供有償對價（包括金錢或其他形式），此有償對價（包括金錢或其他形式）均是為了使用處理服務而提供，而不是為了披露個人資料而提供。除非為了履行處理服務或者存在法律或EULA允許的其他情況，否則資料處理者不得為任何目的保留、使用、披露或銷售個人資料。為免生疑義，除非 EULA 或適用法律另行允許，資料處理方不得出售個人資料，亦不得授權或以其他方式允許任何下級處理者出售個人資料。

附件 2 - 資料處理者實施的安全措施

1. 對場所和設施的物理訪問控制

資料處理者將實施技術和組織措施，以控制對場所和設施的訪問，特別是檢查授權以確保防止未經授權的訪問。

具體如下：

- 門禁系統
- ID讀卡機、磁卡、晶片卡
- 鑰匙發放
- 門鎖
- 保安人員、警衛
- 監控設施
- 報警系統、視頻/閉路電視監視器

2. 對系統的訪問控制

資料處理者將實施技術（ID/密碼安全）和組織措施識別和驗證使用者身份，以防止對 IT 系統的未授權訪問。

具體如下：

- 密碼程式（包括特殊字元、最小長度、密碼更改）
- 自動封鎖（例如，密碼或超時）
- 資料載體的加密，包括可移動和攜帶型資料載體。

3. 對資料的邏輯訪問控制

資料處理者將使用授權方案和訪問許可權的需求驅動定義以及訪問的監控和日誌記錄，以確保阻止未包含在分配的訪問許可權範圍內的 IT 系統活動。

具體如下：

- 基於角色的存取權限（設定檔、角色、交易和物件）
- 使用商業特權帳戶管理解決方案促進管理帳戶對系統的安全身份驗證，以用於維護或其他管理目的
- 定期審查和跟進異常或可疑活動的自動生成報告
- 使用最小權限模型，僅允許基於需要知悉原則存取系統和/或資料

4. 披露和資料保護控制

資料處理者將在資料載體（手動或電子）上傳送、傳輸和交流或存儲資料時採取措施，以及透過電子傳輸、資料傳送和傳輸控制進行後續檢查，從而對個人資料的披露進行控制。

具體如下：

- 加密/隧道
- 電子簽名
- 記錄並持續監控安全事件和警報
- 確保傳輸安全，對傳輸中的資料進行加密
- 靜態資料加密
- 定期輪換加密密鑰
- 僅限有限的人員訪問加密密鑰
- 啟用複雜密碼要求，所有遠端訪問會話都需要兩重因素身份驗證

5. 輸入控制

資料處理者將維護資料管理和維護的完整文檔，包括後續檢查資料是否已輸入、更改或清除（刪除）的相關措施，以及關於由誰實施輸入、更改或清除（刪除）的記錄文檔：

具體如下：

- 記錄和報告系統

6. 作業控制

資料處理者將根據資料控制者的指示處理個人資料，並同意採取（技術/組織）措施以分離資料控制者與資料處理者之間的職責：具體如下：

- 合同措辭明確
- 正式除錯（申請表）
- 選擇資料處理者的標準
- 監督合同履行

7. 可用性控制

資料處理者將採取措施確保資料的物理和邏輯安全性，確保資料免遭意外或惡意破壞或丟失。

具體如下：

- 備份程式
- 硬碟鏡像，例如 RAID 技術
- 不間斷電源（UPS）
- 複製到備用資料中心的遠端或基於磁碟的存儲
- 定期更新的防病毒和/或反惡意軟體以及使用預設拒絕語句配置的應用程式感知防火牆系統，僅允許明確許可用於業務目的的流量
- 業務連續性和災難恢復計劃

8. 隔離控制

資料處理者將透過實施特定措施，為不同目的對資料進行單獨處理（存儲、修改、刪除、傳輸），以確保為不同目的收集的資料將被單獨處理，而不會與其他客戶資料混合：

具體如下：

- 「內部客戶」概念/使用限制
- 職能分離（生產/測試）